Notes (03/07/2024)

Less like notes, more like a glossary of terms in tech class.

1. **White Hat Hacker** - An ethical computer hacker who specializes in penetration testing and vulnerability assessments to identify and fix security flaws. They work for companies/organizations with permission.
2. **Black Hat Hacker** - A malicious hacker who breaks into computer systems with criminal motivations like stealing data or causing disruption. They work illegally for personal gain.
3. **Gray Hat Hacker** - A hacker who may violate ethical standards or laws but without malicious intent. Their motivations can be a mix of good and bad.
4. **Gold Hat Hacker** - A hacker who breaks into systems as a challenge to expose and highlight security vulnerabilities, sometimes leaking data.
5. **Hacktivism** - The act of hacking, or breaking into a computer system, for a politically or socially motivated purpose.
6. **Anonymous** - A decentralized international hacktivist group that conducts cyber attacks against governments, corporations, and others as a form of civil disobedience and activism.
7. **Julian Assange** - Founder of WikiLeaks who published classified information exposing governmental abuses and secrets, making him a key figure in hacktivism.
8. **WikiLeaks** - A non-profit that publishes classified information leaks and news exposing oppressive regimes and corporate wrongdoing.
9. **Edward Snowden** - Former NSA contractor who leaked classified documents revealing global surveillance programs by U.S. and U.K. intelligence agencies.
10. **Malware** - Malicious software designed to gain unauthorized access or cause damage to a computer system.
11. **Virus** - A type of malware that self-replicates by inserting its code into other programs.
12. **Trojan** - Malware disguising as legitimate software that gains unauthorized access once activated.
13. **Adware** - Malware that automatically renders advertisements to generate revenue for its creator.
14. **Ransomware** - Malware that encrypts data and demands ransom payment to restore access.
15. Cyberattack - An assault on computer systems, networks or infrastructure to disrupt, disable, destroy or maliciously control.
16. **Brute Force Attack** - Attempting to guess credentials like passwords or encryption keys through exhaustive effort.
17. **DDoS Attack** - Overloading a targeted system with a flood of internet traffic to disrupt or crash services.

18. **Exploit** - Code that takes advantage of a software vulnerability to penetrate a system.
19. **Vulnerability** - A flaw in software, hardware or procedures that creates a security risk.
20. **Social Engineering** - Manipulating or tricking people into revealing sensitive information or bypassing security measures.
21. **Phishing** - A type of social engineering attack that uses fraudulent emails, texts or websites to trick victims into revealing sensitive data.
22. **Spamming** - Sending unsolicited bulk messages indiscriminately for purposes like phishing or spreading malware.
23. **Sniffing** - Using software to monitor network traffic and capture data packets to steal information
24. **Telephone Spoofing** - Disguising the caller ID information to impersonate a trusted entity during social engineering attacks.
25. **Web Spoofing** - Creating a fake website that is visually identical to a legitimate one to steal user data.